AMENDMENTS TO THE CLAIMS:

This listing of the claims will replace all prior versions, and listings, of the claims in this application.

Listing of Claims:

1. (Currently Amended) A method, comprising:

performing an automated security scan of a second network device by a first network device to determine ~~a~~ at least one of a hardware or software capability of the second network device;

determining an attribute for the second network device based, in part, on the determined capability;

generating an attribute certificate for the second network device based in part on the attribute;

storing the attribute certificate including the attribute on a device other than the second network device; and

responsive to a verified authentication request from the second network device for access to a resource over a network, determining ~~that~~ whether the stored attribute certificate for the second network device is valid, ~~and~~ where if the stored attribute certificate is determined valid, authorizing access to ~~a~~ the resource over ~~a~~ the network based, in part, on the attribute associated with the attribute certificate, or else denying access to the resource for the second network device.

2. (Canceled).

3. (Original) The method of claim 1, wherein the attribute is further determined based, in part, on a condition to be satisfied.

4. (Original) The method of claim 1, wherein the attribute is further associated with a group of network devices.

5. (Original) The method of claim 1, wherein the attribute is further associated with a group of users.

6. (Previously Presented) The method of claim 1, wherein the attribute certificate is generated by at least one of the first network device, an access server, and an attribute authority.

7. (Currently Amended) The method of claim 1, wherein the attribute certificate is stored in ~~at least one of the second network device, and~~ an attribute repository.

8. (Original) The method of claim 7, wherein the attribute certificate is provided to an access server through the use of at least one of a cookie, a program, and a manual upload.

9. (Currently Amended) An apparatus, comprising:

an interface configured to perform an automated security scan of a network device to determine ~~a~~ at least one of a hardware or software capability of the network device;

a processor configured to determine an attribute for the network device based, in part on the determined capability;

the processor further configured to generate an attribute certificate for the network device based, in part, on the attribute;

a memory configured to store the attribute certificate including the attribute on a device other than the network device; and

responsive to a verified authentication request from the network device for access to a resource over a network, the processor further configured to determine ~~that~~ whether the stored attribute certificate for the network device is valid, ~~and~~ where if the stored attribute certificate is determined valid, the processor is configured to authorize access to ~~a~~ the resource over ~~a~~ the network based, in part, on the attribute associated with the attribute certificate, or else to deny access to the resource for the network device.

10. (Previously Presented) The apparatus of claim 9, wherein the processor is further configured to generate the attribute certificate based on a condition to be satisfied.

11. (Canceled).

12. (Previously Presented) The apparatus of claim 9, wherein the processor is further configured to generate the attribute certificate based on the automated security scan of the network device.

13. (Currently Amended) The apparatus of claim 9, wherein the interface is further configured to send the attribute certificate to ~~the network device~~ an attribute repository to be stored.

14. (Currently Amended) A device for managing authorization to a resource over a network, comprising:

means to perform an automated security scan of a network device to determine ~~a~~ at least one of a hardware or software capability of the network device;

means for determining an attribute for the network device based, in part, on the determined capability of the network device;

means for generating an attribute certificate for the network device, wherein the attribute certificate is based in part on the attribute;

means for storing the attribute certificate on a device other than the network device; and

means responsive to a verified authentication request from the network device for access to a resource over a network for determining ~~that~~ whether the stored attribute certificate for the network device is valid, ~~and~~ where if the stored attribute certificate is determined valid, means for authorizing access to ~~a~~ the resource over the network based, in part, on the attribute associated with the attribute certificate, or else for denying access to the resource for the network device.

15. (Previously Presented) The device of claim 14, where the means to perform an automated scan comprises an interface; and the means for determining, generating, storing, and means responsive comprises a central processing unit coupled to the interface and further coupled to a memory.

16. (Currently Amended) A computer readable medium encoded with a computer program executable by a processor to perform actions comprising:

performing an automated security scan of a network device to determine ~~a~~ at least one of a hardware or software capability of the network device;

determining an attribute for the network device based, in part, on the determined capability;

generating an attribute certificate for the network device based in part on the attribute;

storing the attribute certificate including the attribute on a device other than the network device; and

responsive to a verified authentication request from the network device for access to a resource over a network, determining ~~that~~ whether the stored attribute certificate for the network device is valid, ~~and~~ where if the stored attribute certificate is determined valid, authorizing access to a resource over a network based, in part, on the attribute associated with the attribute certificate, or else for denying access to the resource for the network device.